ISO/IEC JTC 1/SC 27/WG 3 N 477

ISO - International Organisation for Standardisation
IEC - International Electrotechnical Commission

JTC 1 - "Information Technology"
SC 27 - "Security Techniques"
WG 3 - "Security Evaluation Criteria"

TITLE:	Disposition of comments (1.0) – A framework for IT Security assurance (Draft 3.0)
SOURCE:	WG 3 Meeting, Madrid, Spain, April 1999
DATE:	1999-04-23
PROJECT:	ISO/IEC JTC 1.27.21
STATUS:	For distribution within ISO/IEC JTC 1/SC 27

Contents

Status and next steps

April 1999

- Acting Editing team assumes duties in April 1999: Mr. Aaron Cohen, Mr. Thomas Gast, Mr. Roland Schützig
- Major reorgianization of the structure of the document to be more readable and presentable. Also new Figure 1 and Table has been created to set the direction for the discussion of assurance methods.
- Address the disposition of comments. Plan way forward to CD in October 2000
- Writing tasks assigend to editing team to reorganize document.
- Defining the needs for detailed input
- Call for expert input from national bodies
- Request for CD extension of one year for October 2000
- Justification: transition from previous editor to new acting editing team, reorganization of the document to make it more readable, new ressources now available because of less ressources needed for 15408.
- Plenary April 1999: ask for more participation for FRITSA

Between April 1999 and October 1999:

- Draft available in July 1st 1999
- Expert Input expected

October 1999

- Review document structure and work tasks
- Review comments from national bodies.
- Defining the needs for detailed input
- Reminding the national bodies for the need of expert input
-

October 1999 to April 2000

Expert Input expected
Draft of document avaiable in 15th January 2000.

April 2000

- Review comments and input from national bodies.
- Final work plan for CD preparation

April 2000 to October 2000

- Next Draft available July 1st 2000

October 2000

- Address all comments and modifications as needed (presumably small comments) for CD submission

Expert Input needed

The response of the editors to comments may result into the need for more expert input. This is indicated in the text with the term „needed input“ and in the left column with the abbreviation „**NfI**“.

The following comments contain a need for expert input:
T11,12, 14, 15, 18
G 6, 7, 14, 15, 16, 19, 21, 22, 23, 29, 30, 31, 32, 33, 34, 36, 37, 38, 40, 41

Note: Use of the table of comments:

- The table contains an identification of the comments in the left column.
- The table reproduces each individual comment without change in the right column.
- The editor’s responses to the comment is given directly following each comment.

Canadian NB Comments

There are 22 canadian comments, numbered T1-T18 and E1-E4.

<table>
<tr><th>Major Technical</th><th>Comment</th></tr>
<tr><td>T1</td><td>ALL
The document must be reviewed to ensure that the information is relevant to the current thinking on assurance methods and to remove the bias to evaluation assurance. Additional information is required on assurance methodologies other than Evaluation Assurance.</td></tr>
<tr><td colspan="2">The comment is accepted. The objective of the document will be to define possible assurance approaches and to define the relationships between the identified approaches including evaluation assurance.</td></tr>
<tr><td>T2</td><td>P4 C5.1
Editors note - "Assurance as a measure of trust” should not be used since the word trust has a lot of baggage and people do not use it properly. Suggest using the word confidence in place of trust.</td></tr>
<tr><td colspan="2">The comment is accepted. The word trust will be avoided. The editor’s note concerning the alignment with the ISO/IEC 15408 usage will be followed.</td></tr>
<tr><td>T3</td><td>P5 C5.1
The first sentence should be changed top read "Assurance is a measure of the confidence in a system to perform in the way intended".</td></tr>
<tr><td colspan="2">The comment is accepted. Editor’s proposal would be to change the first sentence to „Assurance is grounds for confidence that an IT product or system works in the way intended by meeting its security objectives.“</td></tr>
<tr><td>T4</td><td>P5 C5.1
Delete the word "advertised" as it is not appropriate. The word ”advertised” is associated with marketing and assurance is not a measure of how well the vendor markets the product or system. The word ”claimed” could possibly be used in place of the word ”advertised” if the Editor sees fit.</td></tr>
<tr><td colspan="2">The comment is accepted. The word „advertised“ will be changed to „claimed“.</td></tr>
<tr><td>T5</td><td>P5 C5.1
This sentence must be modified because confidence is more than being ”based on experience through actual usage” (note that usage is a form of testing, albeit informal). Confidence is also not necessarily ”a measure of the end-users perception of assurance”. Confidence can be achieved at every abstraction level and by more than the end-user. For example, evaluators will assign an assurance rating based on their confidence of the product satisfying the criteria and certifiers will publish a report stating their findings and a statement indicating the confidence they have given the findings. Users may select a product based on their confidence gained by examining the product implementation documents, testing documents, and/or a third party report such as an evaluation report. Suggest that the sentence be changed to ”Confidence is the belief that the product or system will perform as intended based on the knowledge gained from an assurance method which may include testing”.</td></tr>
<tr><td colspan="2">The comment is accepted. Editor’s proposal: Testing should not be appointed from any assurance method. The sentence will be changed to ”Confidence is the belief that the product or system will perform as intended based on the knowledge gained from an assurance method”.</td></tr>
<tr><td>T6</td><td>Figure 1
Suggest that the figure be reviewed and presented differently with an expanded explanation. If the figure is not changed it must be modified to contain the assurance approach in the intersecting circles to demonstrate the common attributes. Also additional text is required to</td></tr>
</table>

<table>
<tr><td></td><td>explain that these approaches within the circles are specific instances of the large circles and that these 4 assurance approaches are NOT the only assurance categories and there are also many more assurance approaches than listed in the circles.</td></tr>
<tr><td colspan="2">The comment is accepted. See reference German NB comments G12..</td></tr>
<tr><td>T7</td><td>Figure 1
This figure needs to be reviewed and changed so as not to be so limiting. Currently, this figure defines 4 assurance approach categories and leaves no room for growth. Since this is still a new area, the figure should be redrawn so as to accommodate new assurance approaches, otherwise, there will be a problem of fitting square pegs in round holes when a new assurance approach does not fit cleanly into these assurance categories. This situation will occur when an assurance approach is different than the predefined assurance approach categories or the assurance approach overlaps multiple assurance approach categories thereby causing 2 camps of people with different views. Additionally, many assurance approaches combine different assurance elements and aspects of other assurance approaches, which will complicate classifying the assurance approach.</td></tr>
<tr><td colspan="2">The comment is accepted. See reference German NB comments section G12.</td></tr>
<tr><td>T8</td><td>Table1
Add note to Table 1: ”Canada and the USA both had ad-hoc TPEP assessment processes which were never formally documented”.</td></tr>
<tr><td colspan="2">The comment is accepted. Details will be described in a related subsection.</td></tr>
<tr><td>T9</td><td>Table1
Replace the ”?” for SSE-CMM with SSAM, for ISO 9000 with ISO 9000, and CC with CEM. Add a note that these assurance schemes (CC and SSE-CMM) are expected to address the maintenance method as well.</td></tr>
<tr><td colspan="2">The comment is not accepted. For instance CEM and ITSEM are evaluation manuals, not assurance schemes. But Table 1 will be reviewed (in accordance with the German comments) and aligned with actual facts.</td></tr>
<tr><td>T10</td><td>Table 1
The actual name for the assurance scheme for CEM may be different between countries. Suggest that CEM and ITSEM are valid names for their respective assurance schemes and insert a note that these assurance schemes are used since that is what was known at the time of writing.</td></tr>
<tr><td colspan="2">The comment is not accepted. See T9: CEM and ITSEM are evaluation manuals, not assurance schemes.</td></tr>
<tr><td>T11
NFI</td><td>T11 Table 1
Suggest that ”Audit” is the assurance scheme for ISO 9000.</td></tr>
<tr><td colspan="2">The comment is not accepted. Audit is a method, which may be conducted within any scheme. See German comments concerning ISO 9000 scheme:
ISO 9000 AssessorCertification is done by national certification bodies like the DGQ
ISO 9000 Assurance Scheme is provided by national certification bodies like the DGQ
But Table 1 will be reviewed and aligned with given scheme names/certification bodies where available.</td></tr>
<tr><td>T12
NFI</td><td>P10 C5.6&7
Composition of assurance approaches must be expanded to identify which assurance approaches are similar and provide insight on trade-offs between the different approaches. This will help authorities and end-users to minimize the burden for an organization to achieve an assurance capability or multiple assurance capabilities. This will also result in reducing the time and cost to achieve an assurance capability.</td></tr>
<tr><td colspan="2">The comment is accepted. The composition of assurance approaches must be expanded (may be not in this central document but in an annex or separate part of 15443. A needed input will be created to do this work, because the information to do this is not available to the editor at this time.</td></tr>
<tr><td>T13</td><td>T13 P11 C6.1
Disagree with Editors note. This document is too immature to explore this direction at this time. ISO/IESC CD 15408-3 (Common Criteria - CC) contains a strict framework and will bias the assurance framework towards evaluation assurance. The working group needs</td></tr>
</table>

<table>
<tr><td></td><td>time to determine the appropriate assurance framework without being tied to a particular one such as evaluation assurances. Once there is an acceptable structure defined or if no other one seems appropriate, then it will be time to examine more closely how the assurance framework relates to the CC (this will also serve as a kind of QA check of the CC assurance). Remember that the framework is for more than TOE evaluations and the CC assurance is focused (at the moment) solely on evaluations.</td></tr>
<tr><td colspan="2">The comment is accepted. Once the document is more mature, we will explore alignement with ISO standards (in particular 15408).</td></tr>
<tr><td>T14
NFI</td><td>C7.1
Agree with Editor’s note. This must be fixed. See above comment.</td></tr>
<tr><td colspan="2">The comment is accepted. The relationship of assurance approaches will be expanded (may be not in this central document but in an annex or separate part of 15443). A needed input will be created to do this work, because the information to do this is not available to the editor at this time.</td></tr>
<tr><td>T15
NFI</td><td>C7
Section 7 requires significant work to capture the essence of the various assurance approaches and to determine the common elements to be able to facilitate comparison between the different approaches. A relationship is the only feasible direction to take at the moment since a
Numerical analysis is premature due to the lack of understanding of assurance at this time.</td></tr>
<tr><td colspan="2">The comment is accepted. See T14.
The relationship of assurance approaches will be expanded (may be not in this central document but in an annex or separate part of 15443). A needed input will be created to do this work, because the information to do this is not available to the editor at this time.</td></tr>
<tr><td>T16</td><td>Section 3.7 in WD 15443
Change the definition to include ”an assessment of functionality and assurance”. Suggested rewrite ”An assessment of IT product or system functionality and assurance against defined criteria”.</td></tr>
<tr><td colspan="2">The comment is not accepted. The given definition of evaluation is the well used and well known definition used in ITSEC/CC and CC/CEM. This defintion should not be changed.</td></tr>
<tr><td>T17</td><td>6.1
Agree with Editor’s note</td></tr>
<tr><td colspan="2">The comment is accepted and is in contradiction to T13. 15408 terminology will be used in 15543 as far as possible.</td></tr>
<tr><td>T18
NFI</td><td>8-10
These sections must be completed</td></tr>
<tr><td colspan="2">The comment is accepted.
The application of metrics will be expanded (may be not in this central document but in an annex or separate part of 15443). A needed input will be created to do this work, because the information to do this is not available to the editor at this time.</td></tr>
<tr><td>E1</td><td>3 4
AAWG definition should be ”assurances Approaches Working Group (Common Criteria Project)”</td></tr>
<tr><td colspan="2">The comment is accepted, if this is the official name of the CC AAWG, which must be validated.</td></tr>
<tr><td>E2</td><td>3 4
CTCPEC definition should be ”Canadian Trusted Computer Product Evaluation Criteria” - Change ”program” to ”criteria”</td></tr>
<tr><td colspan="2">The comment is accepted. „program“ will be changed to „criteria“.</td></tr>
<tr><td>E3</td><td>3 4
Add definition ”SSAM - SSE-CMM Appraisal Methodology”</td></tr>
<tr><td colspan="2">The comment is accepted. The editor needs information from the originator of the comment about SSAM.
In addition CEM should be added to the list.</td></tr>
<tr><td>E4</td><td>11 6.1
Figure 2 needs to be cleaned up</td></tr>
</table>

The comment is accepted. See german comments. Figure 2 will be reviewed.

German NB Comments :

There are 41 german comments, numbered G1 to G41.
For each comment the respective location in WDTR 15443 will be given for reference.

<table>
<tr><th>Reference</th><th>Comment</th></tr>
<tr><td>G1
General comment
Introduction</td><td>The paper presents a very interesting and very important approach to specify and compare the various methods in information technology security assurance. It seems worth to work at this paper with the aim to harmonize the several approaches to gain efficient assurance methodologies by senseful combination of the specified approaches.</td></tr>
<tr><td colspan="2">Accepted. No action required.</td></tr>
<tr><td>G2
General</td><td>This section provides comments which refer to the overall structure of the document or which are otherwise not specific or local to specific section of the document.</td></tr>
<tr><td colspan="2">Explanation to the structure of the comment paper. No action required</td></tr>
<tr><td>G3
Editorial,
sect. 5.4</td><td>The section 5.4 is basically a starting point to describe various assurance schemes. In order to better reflect the hierarchy
• Assurance approach
• Assurance method
• Assurance scheme
in the overall structure of the document, we recommend to move section 5.4 behind section 6 and make a new section 7 of it. There will be more to tell about the existing schemes. That will cause the section to become larger anyway.</td></tr>
<tr><td colspan="2">Accepted. The overall structure of the document will be improved.
The structure
• Section 1 Scope
• Section 2 References
• Section 3 Terms and definitions
• Section 4 Abbreviated terms
• Section 5 Assurance framework (introducing “assurance approaches”)
• Section 6 Assurance Methods
• Section 7: Assurance Elements
• Section 8: Metrics
• Section 9: Assurance Schemes and Recognition
• Section 10: Relationships between Assurance Methods
• Section 11: Guidance
  • 11.1 Guidance on application of specific assurance methods
  • 11.2 Composition of Assurance Methods
  • 11.3 Recommendation: How to achieve recognition of assurance derived from composition of assurance methods
(Note: Section 7 contains what was originally in section 5.5. The term assurance activitiy was introduced to replace the forme term assurance element in order to avoid conflicts with WD15408. A better term might be needed.)</td></tr>
<tr><td>G4
Editorial
Sect. 6/7/8</td><td>The documents begins to become unreadable more and more. We recommend to separate details of any assurance approach, assurance method or assurance schemes or relationships in annexes. The main sections
• 6 (description of assurance methods)
• 7 (description of assurance schemes)
• 8 (description of relationships)</td></tr>
</table>

<table>
<tr><td></td><td>should only provide essential overviews (say up to one page for each item discussed, e.g. a specific method or issue).</td></tr>
<tr><td colspan="2">Accepted. Annexes will be included in the document for assurance methods, assurance schemes, relationships and metrics, …
Editorial details will be aligned with given ISO rules where applicable.</td></tr>
<tr><td>G5
Editorial
Sect. 1</td><td>Of course we may <i>consider</i> any method in the context of ISO/IEC 15408. But it should be clear to everybody, that it is not ISO/IEC 15408, which gives us the framework. ISO/IEC 15408 is a typical ”system approach (to assurance)”, as it is coined in sect. 5.3 of the assurance framework. As such ISO/IEC 15408 may serve as the ”reference model” for verifications of other kind.
The assurance framework should take in a much broader view on the assurance problem than ISO/IEC 15408 did ever intended.
<b>Recommendation</b>: Change the wording of the third paragraph in section 1 to: ”Each assurance method should be considered in the context of the ISO evaluation criteria [ISO/IEC 15408], to identify the relationship to this reference and the degree of compatibility.</td></tr>
<tr><td colspan="2">Not Accepted. Compare with T13 above.
However, wording will be changed. Each assurance method will be considered to identify the relationships whether they are standards or not. Existing standards/criteria and standards in development such as ISO9000, 15408, ITSEC etc. will be considered. Any other non ISO standards will be considered.</td></tr>
<tr><td>G6
Editorial
Sect. 2
<b>NFI</b></td><td><b>Additional References</b>:
• Dealing with alternative assurance approaches, the assessment of software processes should be considered referencing ISO/IEC 15504 Software Process Assessment.
• Dealing with the measurement and rating of assurance, the activities of SC7 WG 13 should be considered referencing ISO/IEC WD 15939 Software Measurement Process Framework.
• The German V-model could be considered and referenced.
• Dealing with testing, the ISO/IEC 9646 Conformance testing methodology and framework should be considered and referenced.
• Dealing with evaluation ISO/IEC 14598 Software product evaluation should be referenced.</td></tr>
<tr><td colspan="2">Accepted. The precise references have to be determined and will be included in the reference list.</td></tr>
<tr><td>G7
editorial
Sect. 3
<b>NFI</b></td><td>In the definition of <b>assessment</b> the term <b>verification</b> is used, which does not fit the regular definition of verification in the scope of software engineering. What is the referred definition of <b>verification</b>?
Another well used definition of <b>assessment</b> is as follows:
<b>Product Assessment</b> is the action of applying specific documented assessment criteria to a specific software module, package, or product for the purpose of determining acceptance or release of the sofware module, package or product.
There also exist a seperation of software product assessment and software process assessment. That’s why a specific definition is used for software process assessment:
<b>Process Assessment</b> is an evaluation of an organization’s software processes against a process model.
The definition of <b>certification</b> is focused on the certification of installed systems, which seems to be the definition of <b>system accreditation</b>. A more open and more feasible definition is provided by the ITSEC:
<b>Certification</b> is the issue of a formal statement confirming the results of an evaluation, and that the evaluation criteria used where correctly applied.
ISO 9000 provides another useful definition of certification:
<b>Certification</b> is the procedure by which a third party gives written assurance that a product and/or service, process or quality management system conforms to specified requirements.</td></tr>
<tr><td colspan="2">Accepted.
The term “verification” will not be used to denote “assurance approaches” or “assurance methods” any more in order to avoid conflicts with given terminology in software engineering.
The proposed definitions for “product assessment”, “process assessment” and “certification” will be included in the glossary.</td></tr>
</table>

<table>
<tr><td colspan="2">The currently given text for the definition of “certification” (sect. 3.6 in WDTR 15443) will be kept but used instead to define the term “system accreditation”.
Also the editors recognize the need for telling the sources of definitions within the glossary section. This will give a new needed input.</td></tr>
<tr><td>G8
Technical
Sect. 3</td><td>Any term we may use to denote a certain assurance approach will be already in use in a certain context (say SW engineering for example). The glossary should introduce any term as ”xyz approach to assurance” and any us of the terms in the document should be accordingly. This may make it sufficiently clear, that these terms are used solely for the purpose of categorising the multitude of available methods, each founding assurance in IT.
If these terms are used this way throughout the document, there shouldn’t be any confusion any more, as the reader knows, that these terms in the given combination now bear a <b>certain defined meaning in the assurance framework</b>.</td></tr>
<tr><td colspan="2">Accepted. A review of the term assurance approache will be done. See German NB comment G12.
New terms coming out of this will be included in the glossary.</td></tr>
<tr><td>G9
Technical
Sect. 3</td><td>There are methods to evaluate an IT system with respect to it’s technical security properties without having a specific operational environment in mind. While the process as such is covered by the term ”evaluation”, the entity subjected to this evaluation is neither a ”system” nor is it a ”product”. The term is implicitly introduced by the definition of ”system”, but should be defined explicitly in order to have a firm basis of understanding when discussion purely technical oriented evaluation methods. Otherwise we wouldn’t have a proper term to denote a complex hardware/software configuration, which may neither be regarded as a product nor as a system.
<b>Recommendation</b>: Introduce the term ”IT Installation” as: ” a configuration of hardware and software, which is made from IT products and may be used as part of a system.”
<b>(A reference for this definition might be found within the ITSEC/ITSEM context. Pending). This causes a new working item.</b></td></tr>
<tr><td colspan="2">Not accepted. There seems not be an immediate need for such a definitions.</td></tr>
<tr><td>G10
Technical
Sect. 5.3</td><td><b>(numbering of details of comments is not part of the original comment paper. It has been introduced in this document for easier reference)</b>
(1) Figure 1 should be improved to indicate exactly those assurance methods, which will be described in section 6.
(2) There seems to be a lot more methods and standards available as Figure 1 indicates right now. In order to have a central reference for all of them and for their relationship within the assurance approaches model, we should will in here additional references as they come up.
(3) In particular, as Process Approaches SPICE/ISO15504 should be included additional to ISO9000.
(4) More Examples:
ISO/IEC 1554, ISO/IEC WD 15939, German V Model -> Process approaches
ISO/IEC 9646, ISO/IEC 14598 -> system approach (to assurance)
(5) Furthermore:
FIPS 140-1 validation -> system approach (to assurance)
IT auditing following COBIT -> system approach (to assurance)
FIPS PUB 31ff, RFC 1281/1244, <b>German BSI/GISA</b> Security handbook -> Operational approach
Various protection profiles -> system approach (to assurance)
(6) Evaluation should not be categorised as a system approach (to assurance). Evaluation is defined as a process that involves verification and validation techniques. A better header for this class of approaches could be <b>System Approach (to assurance)</b> (see below).
(7) The list of assurance approaches a-f from page 7 should be harmonised with the assurance approaches presented in figure 1 page 8. e seems to be covered in section 5.5 as assurance element f process analysis. (see detailed comments in the next comment section below).</td></tr>
</table>

<table>
<tr><td colspan="2">Accepted.
(1) Figure 1 will be updated to reflect exactly those assurance methods which are described in section 6.
(2) As before.
(3) The precise references have to be determined and will be included in the reference list. A respective description should be included in section 6.
(4) As before.
(5) As before.
(6) Renaming of assurance approach will be done (see above reference sect. 4.2)
(7) Harmonization will be done. For the treatment of specific comments to individual assurance approaches, see below (reference sect. 5.3).</td></tr>
<tr><td>G11
Editorial
Sect. 5.1</td><td><b>(numbering of details of comments is not part of the original comment paper. It has been introduced in this document for easier reference)</b>

1. The given characterisation of assurance is based on effectiveness and correctness. A general framework should not forget the aspect of Functional Assurance FA which is common practice in schemes using conformance testing.
2. The three aspects ”effectiveness”, ”correctness” and ”functional assurance” provide a means to categorise various assurance activities (= the former assurance ”elements”, see sect. <b>Error! Reference source not found.</b> below). They also provide a basis for metrics.
3. This way used these three ”aspects” should no be confused with ”assurance approaches” as they are introduced later.</td></tr>
<tr><td colspan="2">Ad 1. Accepted. The functional assurance aspect will be introduced and related to effectiveness and correctness as appropriate.
Ad 2.: accepted. Approved.
Ad 3.: accepted. No we won’t confuse these „aspects“ with the overall frame work („assurance approaches“, „target of assurance“).</td></tr>
<tr><td>G12
Technical
Sect. 5.3</td><td><b>(numbering of details of comments is not part of the original comment paper. It has been introduced in this document for easier reference)</b>

(This section is a general comment on the assurance approaches. Specific comments on the approaches (a) – (f) will be given subsequently.)
The definition and actual use of the term ”assurance approach” started to become somewhat blurred (see above). Given definitions at various places (starting with the glossary) are not consistent any more. This is also indicated by the introduction of two additional assurance approaches (e) and (f) in section 5.3. These ”new” approaches were actually not missing but are already part of the already existing approaches (see below).
We recommend to clarify the meaning of ”assurance approaches” in section 5.3. That means to clarify
• What an ”assurance approach” is in a generic sense (what sort of category is this?) and
• Which different assurance approaches are available.
•
In order to do so we provide the following recommendations:
(1) Throughout the document the term ”assurance approach” should be used precisely (no other combination of ”approach” with other terms leading to confusion).
(2) The document should be careful reviewed with respect to the proper use of the terms ”assurance approach”, ”assurance method”, ”assurance activity”.
(3) Improve the definition in sect. 3.2 as: ”Assurance approach” <b>-</b> A general concept outlining the direction to be taken to obtain assurance.
(4) Introduce <b>explicit</b> definitions of the specific assurance approaches used in the document in section 5.3 first. Any additional ”definitions” or ”characterisations” of the nature of ”assurance approaches” in general or the specific assurance approaches proposed should be given afterwards (in section 5.3).
The assurance approaches should not be directly life cycle related. This will soon lead to the neat of more ”approaches” seemingly forgotten so far. Instead they should reflect a more general and more independent understanding by just pointing out where to look for the sources of assurance: people, processes, the piece of IT itself, and the use of IT. This</td></tr>
</table>

<table>
<tr>
<td></td>
<td>way the similarity of given assurance methods can be expressed much better.
The coverage of the assurance approaches should be specified by pointing out the assurance elements which are most important or characteristic for the respective approach. For instance configuration management could be part of approach a and b.
Explicit definitions of assurance approaches should be given as follows:

<b>”Personnel and organisation approach (to assurance)”</b>:
The concept of gaining assurance by <b>looking at persons and organisations</b> involved in any assurance activity related to an IT system. This includes for example persons and organisations involved in specification, development, testing, evaluation, certification.

<b>”Process approach (to assurance)”</b>
The concept of gaining assurance by <b>looking at processes</b> which contribute to building or installing security in an IT system. This includes for example processes related to SW development, system integration and maintenance.

<b>”System approach (to assurance)”</b>
The concept of gaining assurance by <b>looking at the IT system</b> at hand itself (either a general IT product or combination of products or an individual IT installation). This includes for example formal evaluation of products, reviewing of the design of systems, testing and technical auditing of systems.

<b>”Operational approach (to assurance)</b>
The concept of gaining assurance by <b>looking at the use</b> of the IT system at hand. This includes any issue of application, administration and day-to-day operation. (Changes and modifications to the IT system should be viewed more under the previous approaches).

(5) Either remove or modify the paragraphs a) to d) in section 5.4 to have them consistent with the somewhat broader understanding of the approaches given above.</td>
</tr>
<tr>
<td colspan="2">This comment is in most parts a rationale supplementing specific comments already given in other reference sections (in particular the following reference sections 5.4 to 5.9).
The document will be carefully reviewed for consistent definition and use of the core terms “assurance approach”, “assurance method”, “assurance scheme”, “assurance element”.
Ad (1): Accepted
Ad (2): Accepted
Ad (3): Basically accepted, but see German Comment G12.
Ad (4): Not accepted.
Discussion in the working group came up with the following categorization of available assurance methods:
There are two dimensions to assurance:
• <b>Assurance approach</b>: whether we look at the „quality“ of processes or at check the results.
• <b>Target of Assurance</b>: whether we look at how secure IT is <b>made</b> or how it is <b>used</b>.

There are two assurance approaches:
• Process approach to assurance:
• Product/system approach to assurance

There are two categories of targets of assurance:
• Design/development oriented assurance
• Operational assurance

These two dimensions will provide FRITSA with a simple 2 by 2 Matrix of four main focuses of assurance. Figure 1 will be revised accordingly. A certain given assurance method may have a focus or primary concern on one or more of those focuses.
These focuses will be used ot give the reader an early understanding of the primary direction of a given assurance method (via Figure 1) and will be used to provide a means to structure section 6, which will describe existing</td>
</tr>
</table>

<table>
<tr><td colspan="2">assurance methods.

Ad (5): Accepted
The editors will remove the paragraphs a) to f) or modify them as appropriate in order make it consistent with the concept introduced above.</td></tr>
<tr><td>G13

Sect. 5.3
approach (a)</td><td>No further comment.</td></tr>
<tr><td colspan="2">No action required</td></tr>
<tr><td>G14
Technical
Sect. 5.3
approach (b)
NFI</td><td><b>(numbering of details of comments is not part of the original comment paper. It has been introduced in this document for easier reference)</b>

(1) It should be made clear that process approaches are the basic of development assurance approaches DA.
(2) Technical Assurance by using state of the art techniques, tools, programming languages etc. should be specified under b. Assurance by the application of general accepted standards and criteria should be discussed under b.</td></tr>
<tr><td colspan="2">Ad (1): Not Accepted at this point of time. We need a definition of DA. -> new needed input.
Ad (2): Approved. That is the very idea of the “process approach”. However, the suggested asspects are reflected by introducing assurance methods under the heading of processs approach to assurance. Of course, these methods should use “state of the art techniques, tools, programming languages etc. and they should represent general accepted standards and criteria. No change of text is needed.</td></tr>
<tr><td>G15
Technical
Sect. 5.3
approach (c)

<b>NFI</b></td><td><b>(numbering of details of comments is not part of the original comment paper. It has been introduced in this document for easier reference)</b>

(1) <b>Verification</b> approaches should be changed to the more general <b>system approach (to assurance)</b> (see above) to avoid confusing interpretations of the several existing definitions of verification and validation.
(2) The difference of assurance gained by first party, second party and third party evaluation should be discussed.
(3) The difference of assurance gained by development integrated, concurrent and consecutive evaluation should be discussed.
(4) Testing assurance should be discussed as an assurance activity (=former ”element”), see below).</td></tr>
<tr><td colspan="2">Ad (1): accepted but also obselete because of new framework, see G12.
Ad (2): accepted. This will give a new <b>needed input.</b> No immediate change of text.
Ad (3): accepted. This will give a new <b>needed input</b>. No immediate change of text.
Ad (4): accepted. “Testing” is an assurance element (activity).</td></tr>
<tr><td>G16
Technical
Sect. 5.3
approach (d)
<b>NFI</b></td><td>The influence of the useability aspect as security functionality to the assurance in operation should be discussed.
The influence of correctness and useability of usage and administration documentation should be discussed.
The ease of use/misuse factor in operational assurance should be discussed.
The way to get evidence of the experience and qualification of the organization and the people should be discussed. The application of accreditation and licencing could be an appropriate way to do this.</td></tr>
<tr><td colspan="2">Accepted. However, Input is needed for that. This will give respective new <b>needed inputs</b>.</td></tr>
<tr><td>G17
Editorial
Sect. 5.3
approach (e)</td><td>We recommend to remove (d) as it is already covered by (a). The current (e) will be the new (d) than.</td></tr>
</table>

Basically accepted, and is considered in the new framework, see G12..	
G18 Technical Sect. 5.3 approach (f)	**(numbering of details of comments is not part of the original comment paper. It has been introduced in this document for easier reference)** (1) The ”system approach to assurance” might easily cover also what is implied in the ”audit approach”, as the ”system approach” is not necessarily confined to the checking of IT products. ”Auditing” of an IT-System implies technical assessment activities. Therefore (f) audit approaches should be changed from a member of the assurance approach list to be a member of the list of assurance elements between f ”process analysis” and g ”testing”. (2) A pure product verification would be near to the development processes also. Thus, question would come up, why this is not encompassed by the ”system approach”. Of course, there is the typical aspect of having an independent third eye performing the evaluation. However, we feel there is no urgent need to make a difference between formal evaluation as a typical system approach (to assurance) for products and a certain IT auditing method (e.g. based on COBIT) an external IT auditor might apply. Both are basically methods to look at piece of IT which ready to use, performed by someone who is often independent from the developer. (3) However, the system approaches to assurance should not be restricted to third party assurance. Third party assurance should be specified as the upper bound of gaining assurance aside first and second party assurance (-> metrics!). Only this way we will have a chance to directly compare formal evaluation methods with audit methods. (4) It is of major importance to gain a ”gridwork” of verification ”elements” as reference for both of them. It will enable us to compare available methods when a ”verification” is to be done for an IT-System, which could be both formally evaluated and audited.
Basically accepted, and is considered in the new framework, see G12..	
Obsolete because of the framework, see G12..	
G19 Technical Table 1 NFI	**(numbering of details of comments is not part of the original comment paper. It has been introduced in this document for easier reference)** (1) CEM and ITSEM are evaluation manuals or evaluation methodologies, not assessment methods. The CC-/ITSEC assessment method is defined as product evaluation. (2) In the CC/ITSEC scheme exists no Assessor & Facility Certification but a facility accreditation including personel licencing. IT-Security Accreditation and Licencing body in Germany is the **German BSI/GISA**. (3) It should be made clear whether **Maintenance Method** means the maintenance of the assessment/evaluation results or means the maintenance of the criteria and the applied scheme. The maintenance method of the criteria CC/ITSEC are the CC/ITSEC Editorial Board CCEB/ITSECEB and the Joint Interpretation Working Group producing the Joint Interpretation Library JIL. (4) CEM and ITSEM are evaluation manuals or evaluation methodologies, not assurance schemes. The CC-/ITSEC schemes are defined by CC-/ITSEC- certification bodies. (5) ISO 9000 Assessor Certification is done by national/international certification bodies like the German DGQ and the EOQ (European Organization for Quality) (6) ISO 9000 Assurance Scheme is provided by national/international certification bodies like the German DGQ and the EOQ (European Organization for Quality) (7) ISO/IEC 15504 Software Process Assessment should be added to the table: • Assurance Method: 15504 • Assessment Method: Assessment • Assessor&Facility Certification: Assessor qualification following 15504 Part 6 • Maintenance Method: tbd • Assurance Scheme: 15504 Part 3 (8) The baseline protection method should be added to the table.

	• Assurance Method: tbd - Code of practice, baseline protection • Assessment Method: tbd - assessment • Assessor&Facility Certification: tbd • Maintenance Method: tbd • Assurance Scheme: tbd (9) ISO/IEC 14598 Software product evaluation should be added to the table. • Assurance Method: tbd • Assessment Method: tbd • Assessor&Facility Certification: tbd • Maintenance Method: tbd • Assurance Scheme: tbd (10) The aspect of useability assurance should be added to the table. (11) It should be formally validated that all identified assurance structures 5.3a-f are covered by the assurance methods in table 1. (12) The requirements of the identified assurance approaches should be mapped anywhere in this paper: ISO9000Part 3 <> CC/ITSEC SPICE <> CC/ITSEC SSE-CMM <> CC/ITSEC ....
Accepted, Table 1 has been restuctured (see Annex 2). Details will be filled in according these comments. Certain details (like references a.o. have to be determined, -> new needed input).	
G20 Editorial Sect. 5.4 Page 9 par 1	such as CSE, NSA, NIST, CESG, **BSI**, **German BSI/GISA** should be added to the list of accreditation bodies.
Accepted	
G21 Technical Sect. 5.5 **NFI**	**(numbering of details of comments is not part of the original comment paper. It has been introduced in this document for easier reference)** (1) Section 5.5 is a starting point to provide a set of ”building blocks”, which can be used to describe any given assurance method. This would be basis for comparing the methods in a structured way by analysing which of those building blocks are contained in a specific assurance method. They could also be the basis for a metric by introducing or using a scaling for each such ”building block”. (2) To begin with this we recommend to rename the section as ”Assurance Activities” in order to emphasise the aspect, that something must be actually done to contribute to assurance. Also there would not be a conflict with the term assurance element in ISO 15408. (However, it is not excluded to identify the assurance activities with ISO 15408 assurance elements at a later point of time.). **We will use in the following the term ”assurance activity” instead of element.** Miscellaneous recommendations (3) In the previous sections of the paper the assurance activities evaluation, audit and assessment are discussed. These assurance activities should also be part of the list. (4) The development activity should be split in development process/method and development environment (technical environment using tools, programming languages and so on). (5) Developers security should be added to the list. (6) As operation is discussed as an assurance activity , configuration should be added to the list. (7) Maintenance including flaw remediation should be added to the list.

<table>
<tr><td></td><td>(8) The assurance activity j) should be removed as it is merely a specific technique.
(9) The assurance activity l) should be removed as it is not a specific assurance activity but a combination or package of activities (or an assurance method?). Anyway, it is a more abstract, i.e. ”larger” concept than any specific ”activity”.
(10) Functional assurance as provided for instance in ITSEC functionality classes and CC protection profiles should be added to the list of assurance approaches.
(11) Section 5.5 is only a starting point for introducing the assurance activities. It is not sure that all the readers of the document understand the meaning of the terms used for the various assurance activities the same way. In order to improve a common understanding we suggest improve each term by a short definition (just a small paragraph) for the beginning. It may look like this, for example:
Personnel: Ensuring that people involved in any activity providing assurance to an IT-System have sufficient expertise, integrity, ...(other qualities) as needed by the nature of their respective contribution. This might include education, training, assessment, licensing.</td></tr>
<tr><td colspan="2">Ad (1): This is just rationales. No specific action required at this place.
Ad (2): not Accepted. We stick to the old term for time being. „Assurance element“ is already defined in CC as the editor’s admit. However, „assurance activity“ might be even more misleading. We look out for a better term.
Ad (3) – (10): Accepted.
Ad (11): Accepted. This will also cause new **needed inputs** in order to get short working definitions of each assurance element.</td></tr>
<tr><td>G22
Editorial
Sect. 5.6
NFI</td><td>Very good discussion! The possibilities for composition of the identified assurance approaches should be specified in this paper. The influence on assurance and efficiency should be identified. This should be the main work on this paper.</td></tr>
<tr><td colspan="2">Accepted.
As stated above in reference sect. 1.1 the restructuring of the document will move this section.
More detailes are needed on this topic as suggested by the comment. This will cause a new **needed input**.</td></tr>
<tr><td>G23
Technical
Sect. 5.1, par 3
NFI</td><td>Within the community of IT auditing (see COBIT for example) the term ”user” is used for those people, which are actually concerned with directly accessing the system (data entry for example). The ultimate responsibility with the ”owner” of a system, who might delegate certain IT control functions to a ”IT custodian”.
We think, that the assurance framework should appeal to the IT auditing people, too. They might be a powerful driver for this effort in the future, when they find out, that this could be valuable tool for them. So, make it more comfortable for them by adopting the term ”IT owner” or ”owner” for the responsible subject.
Recommendation: Use the term ”IT owner” in the 3rd paragraph of section 5.1 instead of ”user”. (This might apply to other locations in the text as well).</td></tr>
<tr><td colspan="2">Accepted.</td></tr>
<tr><td>G24
Editorial
Sect. 6</td><td>Section 6 gives descriptions of available assurance methods. So, the title of the section should tell that accordingly. We recommend to give the title ”Assurance methods” to section 6. At the same time remove sentence 1 of the 1st paragraph in section 6.1.
”Assurance approaches” are just a means to discuss assurance methods and guide their comparison. They may also be used to provide a structure **within** section 6 (as it is basically given now).</td></tr>
<tr><td colspan="2">Accepted: The title of section 6 should be changed to “Assurance methods”. The sentence mentioned in the comment should be removed. Section 6 should be structured into four subsections as indicated by the four assurance approaches. See also G3.</td></tr>
<tr><td>G25
Technical
Sect. 6.1</td><td>**(numbering of details of comments is not part of the original comment paper. It has been introduced in this document for easier reference)**

(1) Section 6.1 bears several different functions as it is given now and is also partly redundant. To make it a real ”overview” (of existing assurance methods) we recommend the following.</td></tr>
</table>

<table>
<tr><td></td><td>(2) Figure 2 is with respect to Figure 1 partly redundant, partly conflicting and also partly inconsistent. We recommend to move Figure 2 to section 8 (former section 7) to an appropriate location, where the specific relationships between developmental assurance and evaluation assurance is discussed.
(3) Refer to Figure 1 in the 1st paragraph of section 6.1 instead of Figure 2. Figure 1 should be improved to indicate exactly those assurance methods, which will be described in section 6. Each assurance method should be put in the respective assurance approach ”bubble”, where its primary focus is.
(4) The Editor’s note refers to ”assurance elements” (or ”assurance activities”, as we recommend to call them, see above). Assurance activities are the basic building blocks of assurance methods. We recommend to move the editor note to section 5.5.</td></tr>
<tr><td colspan="2">Accepted
Ad (1): rationales. No action required.
Ad (2): Figure 2 might be a slight refinement of Figure 1. It will be revised and moved to section 6.
Figure 2 will be harmonized with Figure 1. Additional information gained for specific assurance methods and possibly their relationships as discussed in section 6 may be put into Figure 2. Refinement will still reflect the hierarchy approach/method/activity.
Ad (3): Reference will be changed (see also G12 above).
Ad (4): The Editor’s note will be moved to section 5.5</td></tr>
<tr><td>G26
Editorial
Sect. 6.6</td><td>This section (editor: i.e. sect. 6.6 in WDTR 15443) does not fit into the overall logic of section 6 which describes existing methods, where the section 6 is structured using the identified assurance approaches. We suggest to subsequently identify the different ”assurance activities” being part of ”high reliability assurance methods” and put them into section 5.5 where assurance activities are introduced.</td></tr>
<tr><td colspan="2">It has been decided to move section 5.5 in a main section of its won (section 7, see G3 above).</td></tr>
<tr><td>G27
Editorial
Page 11, Figure 2</td><td>1. The Verification Approaches should be changed to System Approaches (see also comment nr. 2). The discussion in IT-security currently deals with the harmonization of system and process approaches. This must be considered.
2. Why is Software Engineering [Formal Methods] an own bubble? Is Software Engineering not a central part of Developmental Assurance? The intersection between Operational Assurance and Software Engineering should be defined. Is there any one?
3. The position of Audit and Assessment Assurance/Approaches in the presented model should be specified.
4. The position of design and functionality in the model should be specified.
5. There exist intersections between Personnel & Organizational Approaches and the other three bubbles. Or is this bubble restricted to legal aspects? Then the identifier of the bubble should be clarified.
6. A description of the presented model should be given.
7. The role of accreditation, licencing and certification should be added to the model or at least discussed in a description of the model.

<b>(editor’s note: the “comment nr. 2” was part of a previous version of the German NB comment. It is now the reference sect. 5.1 above).</b></td></tr>
<tr><td colspan="2">See G25.</td></tr>
<tr><td>G28
Edtiorial
Sect. 6.2</td><td>As discussed earlier evaluation should not be defined as a verification approach but as a ”system approach to assurance”.</td></tr>
<tr><td colspan="2">Accepted but obsolete. See G12.</td></tr>
<tr><td>G29
Technical
Sect. 6.2.2</td><td>1. In section 6.2.2.1 ”testing” is presented as an element of many kinds of ”assurance approaches”. In fact it is an element of many ”assurance methods”.
2. Section 6.2.2. should be further worked out. Testing is a central aspect in quality assurance and IT-security. Testing approaches should be classified in correctness and security</td></tr>
</table>

NFI	effectiveness tests. 3. There should be specified a scale of assurance beginning with Black Box Tests to White Box Tests with increasing levels from C0-tests to C8-tests. 4. Effectiveness tests should be further specified. Examples of effectiveness tests are for instance fault injection, trojan horse detection, assertion testing, perturbation testing, stress testing, buffer overflow testing and so on. 5. A general test framework should be specified. The qualifiers of the test environments and the test processes should be specified as a precondition to gain assurance by tests. Qualifiers are for instance independency, impartiality (see EN 45001), repeatability and reproducibility. 6. The integration of the test procedures into the development process using several levels of tests as code inspection, module tests, integration tests and acceptance tests should be specified. 7. Beside a test section there should also be included a separate section **Analysis**. Analysis is a key technique in all IT-security evaluation, assessment and audit approaches. Examples of analysis techniques are vulnerability analysis, covert channel analysis, strength of functions analysis, misuse analysis (see Common Criteria).
Ad 1.: Accepted. This section will be removed. Ad 2.: Accepted. Specifics to given methods of conformance testing should be described. This causes a new needed input. Ad 3.: Essentially Accepted. This is new **needed input**. Either this comes along with a given conformance testing method or it has to be elaborated in metrics section. Ad 4.: Accepted. This causes a new **needed input**. Ad 5.: Basically accepted. We expect these details to come with a specific given testing method (or testing scheme) Ad 6.: This is an issue of specific testing methods or methods of developmental assurance (process approach to assurance). Also this may be discussed under the section “relationships between approaches”. This gives cause to a new **needed input**. Ad 7: Not accepted. But it seems as if “analysis” is an assurance element which should be included in section. 7 of WDTR 15443, see G3.	
G30 Technial Sect. 6.3.1 **NFI**	Section 6.3.1. should be further worked out. Developmental assurance is a main aspect in current research activities in the area of alternative assurance approaches.
Accepted. Yes, that is a needed input.	
G31 Technical Sect. 6.3.2.1, page 13, par. 3 **NFI**	Point 2 concerning the SSE-CMM should be described in more detail. The way to get product assurance using SSE-CMM should be described. It should be specified what kind of product assurance can be obtained applying SSE-CMM. The aim of using SSE-CMM to obtain predictable product assurance or to apply assurance activities concering the specific end product should be further worked out.
Accepted: This is a new **needed input**.	
G32 Technical Sect. 6.3.2.1, page 13, par. 4 **NFI**	It should be specified how SSE-CMM minimises the intrusion. Does this mean that SSE-CMM is only built for self assessment? It should be specified how SSE-CMM minimises **unnecessary** documentation. What is meant with unnecessary documentation? The necessary set of documentation should be specified.
Accepted. The sentence refered in the comment has to clarified. This causes a new **needed input**.	
G33 Technical Sect. 6.3.2.1,	The proof of the claims a to c should be delivered.

page 13, par. 5 **NFI**	
Accepted. References or rationales should be provided. This will cause a **needed input**.	
G34 Technical Sect. 6.3.2.2, page 14 par 2 **NFI**	It should be described why SSE-CMM maturity levels L1-L5 do not clearly define the organization maturity. A mapping between SSE-CMM L1-L5 to CC EAL1-EAL7 should be specified. The referred rating profile should be specified.
Accepted. This will cause a **needed input**. The mapping between SSE-CMM and CC (a summary is expected) is part of the current sect. 10 (relationships) and should be described there. Section 6 should describe each assurance method individually.	
G35 Technical Sect. 6.3.3	This section is completely unclear. It should be worked out or should be skipped. For instance it is confusing with other standards to put assurance at the same level with cryptograhic and access control but not to describe access control as one possible class of functionality to gain assurance and cryptographic as one possible mechanism to implement security functionality.
Accepted. This section describes certain techniques and might be included in section 7 (assurance elements).	
G36 Technical Sect. 6.4.1 **NFI**	45001 does not handle certification of personel. 45001 regulates the accreditation of facilities. This facility assurance includes personel assurance. The header of the section should be changed to Facility Assurance or Facility Assurance should be described in an own section.
Accepted. The correct references have to be determined (-> needed input).	
G37 Technical Sect. 6.6 **NFI**	**(numbering of details of comments is not part of the original comment paper. It has been introduced in this document for easier reference)** (1) The described methods are not restricted to reliability. (2) IT-security standards and criteria exist a direct assignment of the use of specification, design, test to the assurance level. The header should be changed. The assignment of methods to assurance should be specified and mapped between the several assurance approaches discussed in this paper. (3) This section 6.6 does not fit into the overall logic of section 6 which describes existing methods, where the section 6 is structured using the identified assurance approaches.
Accepted. There is no need for a specific section to discuss „high reliability“ techniques of its own. These techniques are part of assurance methods and are expressed in assurance elements. The section will be removed. Contents which might be lost than will be moved to section 7. Also it should be renamed to „formal analysis“.	
G38 Technical General, sect. 6.2 **NFI**	It seems to be a good idea to recognise the following hierarchy when discussion assurance approaches: We need assurance about a **system** by performing an **accreditation.** The system is based on an **IT Installation** which may be **assessed** and /or **certified** The IT Installation is a set of **IT products** which may be (formally) **evaluated** and /or **certified** This might not be the best way to establish this hierarchy. The point is: the assurance framework should recognise clearly, that there is a need to assess more complex IT-Installations which may not and need not be treated by formal evaluation. **Recommendation**: As this ”assessment” of IT Installations is a ”system approach to assurance”, this could be worked out also in section 6.2. However, the terminology introduced earlier in the assurance framework could support this understanding.
The concept is basially accepted and will be introduced in section 5 to address the assurance life cycle. See also above for the term “IT-Installation” (G9).	

<table>
<tr><td>G39
Technical
Sect. 7.1 Page 17 Par. 3</td><td>(1) The developer action requirements, content and presentation of evidence requirements of the CC or the ITSEC are not <b>verified</b> during the evaluation but <b>checked</b> or the fulfillment of the requirements is <b>confirmed</b> or <b>determined</b> (see also comment nr. 2).
(2) The evaluator requirements of the CC or the ITSEC are not verified during the evaluation. The evaluator requirements are checked and <b>confirmed</b> by the certifier.</td></tr>
<tr><td colspan="2">Add (1): Accepted. The wording will aligned with CC wording.
Add (2): Accepted. dto.</td></tr>
<tr><td>G40
Technical
Sect. 7.2, 7.3
<b>NFI</b></td><td>1. This section should be worked out in more detail to get the quality of an assurance standard. Otherwise it appears like a position paper generally discussing several assurance approaches without regulating anything in detail.
2. It should not only be discussed how development/process assurance can replace evaluation assurance. It should be discussed how all these assurance approaches can be concatenated to efficient methodologies gaining the same or even comparable assurance levels. It should be specified how process assurance could support product assurance.
3. All development process invariants beside configuration management should be specified. At a first look these are ADO_DEL Delivery Procedures, ALC Life Cycle Support and AMA Maintenance of Assurance. The influence of these process invariants to product assurance should be analysed. It should be checked if the same product assurance is reached by assessing them once and not checking them in each product evaluation process. The effort that could be reduced by pushing the activities from product evaluation to process assessment should be analysed.
4. All operation process invariants should be specified. At a first look this is for instance ASE_ENV Security Environment.
This should be done with all identified assurance approaches a-f from page 7.
It should be specified what evaluation assurance requirements can be replaced by development/process assurance requirements and what evaluation assurance requirements still remain.
5. The DA-approach should be specified before being able to present results as <b>DA methodology may only ... as a low assurance level</b>.
6. DALs should be specified to be mapped to CC EALs.
7. The SSE-CMM, ISO9000,... process assurance requirements should be mapped in detail to the ITSEC/CC product assurance requirements.</td></tr>
<tr><td colspan="2">Accepted. Details have to be worked out. This causes new needed inputs where details are needed as appropriate.</td></tr>
<tr><td>G41
Technical
Sect. 8 Table 2
<b>NFI</b></td><td><b>(numbering of details of comments is not part of the original comment paper. It has been introduced in this document for easier reference)</b>

(1) In section 7 DA and SSE-CCM are discussed as one assurance approach. In section 6 and in table 2 of section 8 they are discussed as two seperate process assurance approaches. This should be clarified.
(2) Assurance 6.3.3 Mulit-party system life cycle control assurance does not appear in table 2.
(3) As Results the metrics <b>reproducibility, impartiality, independency</b> should be added to the list of metrics.
(4) The methodology to apply metrics in assurance should be specified with respect to ISO/IEC WD 15939 Software Measurement Process Framework.
(5) The role of measuring and applying statistics in assurance should be specified.
(6) This framework should specifiy a guidance to solve questions concerning assurance metrics as:
relationship of complexity like Lines of Code and assurance
relationship of evaluation/assurance effort/result and assurance in operation
relationship of number/complexity of security functionality and evaluation/assessment results
relationship of number/complexity of security functionality and assurance in operation</td></tr>
<tr><td colspan="2">Ad (1): “Developmental Assurance” seems to be a category of assurance methods under the heading of “process</td></tr>
</table>

approache (to assurance)”. It includes so far (see WDTR 1553 sect. 6.3.1) ISO9000, SSE-CMM and RAMP).
Ad (2): Table 2 should be improved accordingly (if this is not removed, see reference section. XX.
Ad (3): Add the proposed metrics to the list of metrics reflecting the possible results of measuring processes.
Ad (4): Accepted. This is a needed input.
Ad (5): Accepted. Yes, that is what we need in particular. This is a needed input.
Ad (6): Accepted. Yes, that is what we need in particular. This is a needed input.

US NB Comments :

<table>
<tr><th>Reference (No.)</th><th>Comment</th></tr>
<tr><td>US 1
Editorial
(CR)</td><td>Clause 6.6 - Delete the initial editorial note as incorrect: "this is not an assurance approach/method but a component, this text should be moved".

Rationale - This clause describes controls placed on the development Techniques and forms the fundamental, and most important, assurance method. This is the method that most directly influences the security quality of the IT product or system. The efforts required here of the developer are separate from all other assurance methods. Specifically, evaluation assurance is the production of and confirmation of evidence that developer actions were undertaken. Clause 6.6 is the method that defines what developer actions are to be taken and is independent of the subsequent evaluation of these actions. Clause 6.6 is the definition for the underlying science for producing trustworthy IT.</td></tr>
<tr><td colspan="2">Accepted.
In addition to removing the editorial note as suggested section 6.6 as given now we will move the subject to section 7 (assurance elements), see G3.</td></tr>
<tr><td>US 2
Editorial/Technical</td><td>Clause 7.2, paragraph 1 -
Change: "predictable and repeatable and will therefore yield assurance about the system"
To: "predictable and repeatable and will therefore yield a consistent Level of assurance about the system"

Rationale – Process assurance (which is what this clause is addressing) Speaks to process definition and repeatability, not to the quality of the Engineering being performed. Therefore the key phrase is "consistent level" of quality.</td></tr>
<tr><td colspan="2">Not Accepted. There are two reasons, why the new wording is not correct:
1) Level of assurance is used in evaluation community to refere to precise assurance obtained through evaluation. This type of assurance may not be achievable through an alternative assurance method.
2) Having assurance in the process does not necessarily imply to have assurance or even a certain conistent level of assurance in the specific product or system.
The editor’s propose the following wording:
„…..Predictable and repeatable and will therefore yield a precondition of a consitent assurance of the system at hand.“</td></tr>
<tr><td>US 3
Technical</td><td>Clause 7.2, paragraph 1 -

Change: "Therefore, there is a leap of faith that process assurance implies evaluation assurance: process assurance only implies that which evaluation assurance provides explicitly. It can be easily proven that process assurance will correct errors in the system so that other systems are corrected, however, there is still no direct examination of the system."

To: "Process assurance deals with a consistent, but undefined level of quality, while evaluation assurance verifies a specific level of quality. The development methods described in clause 6.6 actually produce a defined level of quality."

Rationale: Process assurance is about repeatability, not about quality. The assertion that process assurance will correct errors is not correct, as stated. Rather, process assurance is about consistency in the level of quality (or roughly the number of errors). Only the application of the</td></tr>
</table>

<table>
<tr><td></td><td>assurance methods described in clause 6.6 is likely to make s ignificant reduction in the number of errors.</td></tr>
<tr><td colspan="2">The comment is not understood fully. There seems to be a contradiction. Clause 6.6 describes certain process oriented assurance elements. Following the suggested wording, it becomes not clear if process assurance provides an assurance level or not. Clarification is needed.</td></tr>
<tr><td>US 4
Technical</td><td>Clause 7.2, last paragraph – Delete: "The SSE-CMM assurance elements are very similar to the ISO evaluation criteria since the SSE-CMM describes system security engineering practices"
Rationale: SSE-CMM does describe practices (relating to processes, not products), but it does so independently of metrics that produce higher quality process outputs, i.e., products. Evaluation, on the other hand, is specifically about the quality of the products, the process outputs. Process metrics (like SSE-CMM) relate to consistency of processes, not to the quality of the process outputs. It is not a given that consistent processes produce high quality. Rather, consistent processes produce consistent quality.</td></tr>
<tr><td colspan="2">Accepted. However, the editor’s suggest to reword the sentence as follows:
The SSE-CMM assurance elements are mappable to many of the ISO evaluation criteria since the SSE-CMM describes system security engineering practices such as development environment..
We suggest to provide more input, references in order to support that.
The editor’s are aware of the fundamental difference in approaching assurance between process assurance and assurance (see Figure 1).</td></tr>
<tr><td>US 5
(ER)</td><td>Clause 8, last paragraph – Delete: "and how much does it fit in to evaluation?"
Rationale: There is no need to tie all assurance to evaluation. High confidence in the trustworthiness of an IT implementation can be acieved without any evalaution. Evalaution is an after the fact attempt to determine what a developer has done. The ultimate trustworthiness of IT is determined by the developer actions, not by evaluator actions. While both developer and evaluator actions are important, no amount of evaluator action alone can make up for shortfalls in the IT development.</td></tr>
<tr><td colspan="2">Accepted.</td></tr>
</table>

Annex 1: Suggested framework (Figure 1)

Target of assurance: → Assurance approach: ↓	Design/Development/Maintenance („making security“) (D)	Operation („using security“) (O)
Process assurance (P)	SSE-CMM Developer's Pedigree Warranty Assurance Supplier's declaration Personal assurance Evaluation Rating Maintenance ISO 9000	SSE-CMM Personnel Assurance GMITS BSI Code of Practice Baseline Security
Product/system assurance (S)	CC/CEM ITSEC/ITSEM TCSEC CTCPEC Conformance Testing Penetration Testing X/Open Personnel Assurance EN 45000ff	Personnel Assurance

Notes:

1. Personnel assurance should be differentiated to reflect the specific method available in each of those four boxes.
2. The precise titles or names of methods will be included when determined.
3. Additional methods will be included as required.

Annex 2: Suggested improved layout for the table 1

Appr.	Targ.	Assurance Method	Reference No. in sect. 2 or bibliography	Specification of Method	Scheme	Personnel and/or Facility	Maintenance of method
P	D/O	SSE-CMM		Appraisal of organization processes	SSAM (?)	SSO (?)	SSO (?)
S	D	CC/CEM		Product/System Evaluation	Certification schemes ?	Accreditation ?	CCIB/CCEB ?
S	D	ITSEC/ITSEM		Product/System Evaluation	Certification schemes ?	Accreditation ?	Joint Interpretation Group ?
S	D	TCSEC		Product/System Evaluation	TPEP Certification schemes ?	Accreditation ?	?
S	D	CTCPEC		Product/System Evaluation	TPEP Certification schemes ?	Accreditation ?	?
		Conformance Testing					
		Penetration Testing					
		X/Open Branding					
		Personnel Assurance (PA)					
		Developer's Pedigree					
		Warranty assurance					
		Supplier's declaration					
		BSI Code of Practice					
		GMITS					

Notes:

- Details have to be filled in.
- ?-marks denote open references. We need the precise document/stantard/manual etc. referenced here. This will be included in the document where available.